11 / 143-E
2011 07 15

UNCLASSIFIED - For Official Use Only

"Hacktivist" collective threatens Alberta's Oil Sands

KEY POINTS

- On 2011 07 13, Operation Green Rights, self-identified as a project of the "Hacktivist" collective known as Anonymous, published a press release on *YouTube* announcing the beginning of a cyber campaign targeting companies involved in the oil sands industry. The group indicated its solidarity with direct action activists gathered along US Highway 12 in Montana to protest against the transport of refinery equipment to the Alberta, Canada oil sands, and listed various entities against whom it intends to "fight".

- Anonymous has demonstrated that it can effectively mount cyber attacks with the potential to disrupt corporate or government operations. Authorities in Alberta, as well as the RCMP, are aware of the situation.

- ITAC is providing this report to our stakeholders for awareness purposes.

ANALYSIS

1) On 2011 07 13, Operation Green Rights, self-identified as a project of the "Hacktivist" collective known as Anonymous, published a press release on *YouTube* announcing the beginning of a cyber campaign targeting companies involved in the oil sands industry. The group indicated its solidarity with direct action activists gathered along US Highway 12 in Montana to protest against the transport of refinery equipment to the Alberta, Canada oil sands, and listed various entities against whom it intends to "fight". Those entities included "Exxon Mobile, Conoco Phillips, Canadian Oil Sands, Imperial Oil and the Royal Bank of Scotland".

2) The same day, 2011 07 13, Monsanto, a multi-national biotechnology corporation, confirmed it had been the victim of a cyber attack. Anonymous claimed that it took down the company's web site and compromised corporate mail servers, releasing the names, addresses, phone numbers and email addresses of 2500 Monsanto alleged employees.

3) Anonymous gained a high profile beginning in 2010 when the group coordinated a series of attacks against MasterCard, Visa and PayPal following a decision by those companies to cease conducting business with *WikiLeaks* after the publication of thousands of US diplomatic cables. In the same series of attacks, Anonymous also attacked Amazon, but was unsuccessful due to the company's robust online infrastructure.

4) According to open information, in most cyber attacks, Anonymous uses a method referred to as Distributed Denial of Service (DDoS), which consists of directing a large traffic surge to a web site until it becomes overwhelmed and cannot operate efficiently. Depending on the design and capacity of a web site, DDoS attack consequences can range from a slowdown, or speed up to a potential crash of the site. Anonymous also uses a hacking tool known as SQL injection, which consists of exploiting a vulnerable code on a computer system. This allows the hacker to bypass security measures, obtain access to the network and steal information.

5) Authorities in Alberta, as well as the RCMP, are aware of the situation.

6) ITAC is providing this report to our stakeholders for awareness purposes.

ITAC CIET
Integrated Terrorism Assessment Centre | Centre intégré d'évaluation du terrorisme
THREAT L A S E R ALERT

11 / 234-E
2011 10 25

UNCLASSIFIED -
See Handling Instructions

"Anonymous" calls for nuisance activities to coincide with Guy Fawkes Day

KEY POINTS

- On 2011 10 16, the international *hacktivist* group "Anonymous" posted a message online urging sympathizers to participate in a range of nuisance activities targeting governments and media on 2011 11 05 to coincide with Guy Fawkes Day. Dubbed "Operation Injustice Awareness" the call encourages sympathizers to deface web sites and redirect the traffic they receive to "Anonymous" *Twitter* feeds, in keeping with the group's traditional *modus operandi*. The call also encourages sympathizers to take to the streets, wearing Guy Fawkes' masks, to deface their cities with graffiti, to engage anyone who questions them, and to photograph and upload their stories to social media.

- ITAC is providing this report to first responders for situational awareness.

ANALYSIS

1) On 2011 10 16, the international *hacktivist* group "Anonymous" posted a message online urging sympathizers to engage in a range of nuisance activities targeting governments and media on 2011 11 05 to coincide with Guy Fawkes Day (a misinterpreted reference to the British tradition of Guy Fawkes Night, which marks a foiled plot in AD 1605 to assassinate the King of England in which Londoners, rejoicing that their King was safe, joyfully lit bonfires). Dubbed "Operation Injustice Awareness", the call encourages sympathizers to deface web sites and redirect the traffic they receive to "Anonymous" *Twitter* feeds, in keeping with the group's traditional *modus operandi*. The call also encourages sympathizers to take to the streets, wearing Guy Fawkes' masks, to deface their cities with graffiti, to engage anyone who questions them, and to photograph and upload their stories to social media.

2) During the summer of 2011, dozens of "Anonymous" members were arrested in several countries for their attacks on corporate and sensitive government web sites. The group gained notoriety for taking down PayPal and Visa for ceasing to conduct business with *WikiLeaks* after it released thousands of US diplomatic cables. "Anonymous" also took down the web site of Monsanto, a major biotech company, accusing it of being "corrupt, unethical and downright evil". The group has vowed to avenge the arrest of its members.

3) According to open information, in most cyber attacks, "Anonymous" uses a method referred to as Distributed Denial of Service (DDoS), which consists of directing a large traffic surge to a web site until it becomes overwhelmed and cannot operate efficiently. Depending on the design and capacity of a web site, DDoS attack consequences can range from a slow-down, or speed-up to a potential crash of the site. "Anonymous" also uses a hacking tool known as SQL injection, which consists of exploiting a vulnerable code on a computer system. This allows the hacker to bypass security measures, obtain access to the network and steal information.

4) On 2011 10 18, the US Department of Homeland Security (DHS), National Cyber-security and Communications Integration Center (NCCIC), was quoted as saying that the information available on "Anonymous" suggests they currently have a limited ability to conduct attacks targeting Industrial Control Systems (ICS). However, experienced and skilled members could develop capabilities to gain access and trespass on control system networks very quickly. Moreover, free educational opportunities (conferences, classes), presentations at hacker conferences and other high profile events / media coverage have raised awareness to ICS vulnerabilities and have likely shortened the time needed to develop sufficient tactics, techniques and procedures to disrupt ICS.

7) ITAC continues to monitor the situation and will provide updates as necessary.

HANDLING INSTRUCTIONS

This document is the property of the Integrated Terrorism Assessment Centre (ITAC). Prepared by ITAC, it is derived from various sources with information effective as of the date of publication. It is provided to your agency/department in confidence and may be further disseminated by your agency/department to those with the need to know. It must not be reused in any way, in whole or in part, without the consent of the originator. Any feedback should be directed via email to ITAC at or to ITAC Partnerships at

This document constitutes a record which may be subject to mandatory exemption under the *Access to Information Act* or the *Privacy Act*. The information or intelligence may also be protected by the provisions of the *Canada Evidence Act*. The information or intelligence must not be disclosed or used as evidence without prior consultation with ITAC.

ITAC CIET
Integrated Terrorism Assessment Centre | Centre intégré d'évaluation du terrorisme
THREAT L A S E R ALERT

11 / 260-E
2011 11 15

UNCLASSIFIED -
See Handling Instructions

"Anonymous" threatens Toronto with cyber attack

KEY POINTS

- On 2011 11 13, the international collective "Anonymous" posted a video on *YouTube* threatening cyber attacks against the City of Toronto if it follows through with plans to bring the Occupy protest movement "to a peaceful conclusion". In the video, "Anonymous" stated that Toronto would be "removed from the Internet" if the city fails to leave the protestors alone.
- As of 1400 hrs, 2011 11 15, media reporting indicates that Toronto city staff have given eviction notices to Occupy Toronto protestors, saying that protestors must leave the area immediately.

ANALYSIS

1) On 2011 11 13, the international collective "Anonymous" posted a video on *YouTube* threatening cyber attacks against the City of Toronto if it follows through with plans to bring the Occupy protest movement "to a peaceful conclusion". In the video, "Anonymous" stated that Toronto would be "removed from the Internet" if the city fails to leave the protestors alone.

2) "Anonymous" has conducted many successful cyber attacks. For example, in early 2010, the group attacked Australian government web sites with a large Distributed Denial of Service (DDoS) attack. Further, open sources report that the Mayor of St. Louis, Missouri had his emails, political backers, as well as contact information posted online recently by a hacker who claimed to be a member of "Anonymous" after an eviction notice was served to that city's Occupy protestors. There have also been threats made by "Anonymous" that have not materialized, such as a recent claim by the group that they would "erase" the Toronto Stock Exchange (TSX) from the Internet.

3) During the summer of 2011, dozens of "Anonymous" members were arrested in several countries for their attacks on corporate and sensitive government web sites. The group gained notoriety for taking down PayPal and Visa for ceasing to conduct business with *WikiLeaks* after it released thousands of US diplomatic cables. "Anonymous" also took down the web site of Monsanto, a major biotech company, accusing it of being "corrupt, unethical and downright evil". The group has vowed to avenge the arrest of its members.

4) According to open information, in most cyber attacks, "Anonymous" uses a method referred to as DDoS, which consists of directing a large traffic surge to a web site until it becomes overwhelmed and cannot operate efficiently. Depending on the design and capacity of a web site, DDoS attack consequences can range from a slow-down or speed-up to a potential crash of the site. "Anonymous" also uses a hacking tool known as structured query language injection attack, which consists of exploiting a vulnerable code on a computer system. This allows the hacker to bypass security measures, obtain access to the network and steal information.

5) On 2011 10 18, the US Department of Homeland Security (DHS), National Cyber-security and Communications Integration Center (NCCIC), was quoted as saying that the information available on "Anonymous" suggests they currently have a limited ability to conduct attacks targeting Industrial Control Systems (ICS). However, experienced and skilled members could develop capabilities to gain access and trespass on control system networks very quickly. Moreover, free educational opportunities (conferences, classes), presentations at hacker conferences and other high profile events / media coverage have raised awareness to ICS vulnerabilities and have likely shortened the time needed to develop sufficient tactics, techniques and procedures to disrupt ICS.

7) Social media indicates that one means of identifying "Anonymous" individuals or sympathisers may be the wearing of Guy Fawkes masks.

8) ITAC continues to monitor the situation and will provide updates as necessary.

11 / 106-E **CONFIDENTIAL**
2011 06 08

Anarchists call for violent disruption of the Conservative Party National Convention

KEY POINTS

- The 2011 Conservative Party National Convention will take place at the Ottawa Convention Centre from 2011 06 09 to 2011 06 11. The Right Honourable Stephen HARPER, Prime Minister of Canada, will address the convention on the evening of 2011 06 10. Anarchist web sites and social media are circulating an online call for individuals to "fight him (Stephen HARPER) in the streets".

ANALYSIS

1)The 2011 Conservative Party National Convention will take place at the Ottawa Convention Centre from 2011 06 09 to 2011 06 11. Numerous Members of Parliament, past and present, will be in attendance. The Right Honourable Stephen HARPER, Prime Minister of Canada, will address the convention from 1830 hours to 1930 hours on the evening of 2011 06 10.

2) Anarchist web sites and social media are circulating an online call for individuals to "fight him (Stephen HARPER) in the streets". Postings describe this as "direct action" intended to make the laws of the Canadian state "unenforceable", thereby starting a culture of "total rebellion".

3) Of interest, the 2011 06 10 "snake march" is being organized by several multi-issued based groups from Ottawa, Montréal, Vancouver and possibly Toronto, including No One is Illegal (NOI), NOWAR- PAIX and *Convergence des luttes anti-capitalistes* (CLAC). This includes individuals who were involved in violent protest activities during last year's G20 Summit in Toronto, Ontario. Further information posted to anarchist web sites invites anyone who cannot take part in activities in Ottawa on 2011 06 10 to "do something else on the same day or whenever... If you live outside of Canada fight your own government and deprive your enemy of an ally".

4) One of the postings specifically mentioning and inviting hackers to the 2011 06 10 demonstration in Ottawa
Links to the Anonymous group in Canada consist of Canada Anonymous and its active cells Canada Anons and, more locally, the Ottawa Anons and Ottawa Lulz. Canada Anonymous online preparatory site is located at http://filestack.ca.

5) "Anonymous" is an Internet group name that originated in 2003 representing the concept of online community users. Simultaneously existing as an anarchic, digitalized global collective, it has become increasingly associated with international "hacktivism", undertaking protests and other actions often with a goal of Internet freedom and Freedom of Speech. Anonymous members who participate in physical protests are easily identifiable by the wearing of "Guy Fawks" masks, made famous in the movie *V for Vendetta*.

6) More recently, an active Internet-based group loosely affiliated with Anonymous is "Lulzsec". This group has gained media attention recently with a series of high systems intrusions around the world. The Ottawa chapters online can be found at "ottawalulz.com" and "ottawa.wikidot.com". These addresses are currently in "parked domains", meaning there is no information on the site, to date, but they will likely have active content in the very near future.